

This Page Is Inserted by IFW Operations  
and is not a part of the Official Record

## **BEST AVAILABLE IMAGES**

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

**IMAGES ARE BEST AVAILABLE COPY.**

**As rescanning documents *will not* correct images,  
please do not report the images to the  
Image Problem Mailbox.**



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/654,638	09/05/2000	Tsuyoshi Takagi	13700-0251	7659
7590	07/06/2004		EXAMINER	
KILPATRICK STOCKTON LLP 2400 MONARCH TOWER 3424 PEACHTREE ROAD NE ATLANTA, GA 30326			DINH, MINH	
			ART UNIT	PAPER NUMBER
			2132	

DATE MAILED: 07/06/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

<b>Office Action Summary</b>	<b>Application No.</b>	<b>Applicant(s)</b>	
	09/654,638	TAKAGI ET AL.	
	<b>Examiner</b>	<b>Art Unit</b>	
	Minh Dinh	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --  
**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

#### Status

- 1) ☐ Responsive to communication(s) filed on \_\_\_\_.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

#### Disposition of Claims

- 4) ☒ Claim(s) 1-21 is/are pending in the application.  
 4a) Of the above claim(s) \_\_\_\_ is/are withdrawn from consideration.
- 5) ☒ Claim(s) 1-5 is/are allowed.
- 6) ☒ Claim(s) 6-7, 9-12, 14-16 and 18-20 is/are rejected.
- 7) ☒ Claim(s) 8, 13, 17 and 21 is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_ are subject to restriction and/or election requirement.

#### Application Papers

- 9) ☒ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_ is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.  
 Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
 Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

#### Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).  
 a) ☐ All b) ☐ Some \* c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
  2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_.
  3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

#### Attachment(s)

- |   |  |
|---|--|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)   | 4) <input type="checkbox"/> Interview Summary (PTO-413)<br>Paper No(s)/Mail Date. ____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)  | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152)            |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)<br>Paper No(s)/Mail Date <u>3/20/2001</u> . | 6) <input type="checkbox"/> Other: ____  |

Art Unit: 2132

### DETAILED ACTION

1. Claims 1-21 have been examined.

#### *Specification*

2. Claims 1, 9 and 19 are objected to because of the following informalities.
  - a. Regarding claim 1, the preamble is grammatically incorrect.
  - b. Regarding claim 9, "softwares" (third line of claim) needs to be changed.
  - c. Regarding claim 19, "a public keys" and "a secret keys" (third line of claim) need to be changed.

Appropriate correction is required.

#### *Claim Rejections - 35 USC § 102*

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

4. Claims 6-7, 10-12, 14-16 are rejected under 35 U.S.C. 102(b) as being anticipated by Biehl et al. ("Efficient Undeniable Signature Schemes based on Ideal Arithmetic in Quadratic Orders").
  - a. Regarding claim 6, Biehl discloses a method comprising the steps of:

Art Unit: 2132

attaching an undeniable digital signature to a software offered for downloading by clients at a software vendor side (page 1, "In 1989 Chaum and ... they use unmodified software."), according to an undeniable digital signature scheme based on a quadratic field (page 10, see Step 1 for key generation and Step 2 for signature generation); and

carrying out a process of verifying the undeniable digital signature at the software vendor side interactively with each client which has downloaded the software with the undeniable digital signature attached thereto, so as to prove that the software has not been altered from an original (page 11, see Step 3 for confirmation protocol).

b. Regarding claim 7, Biehl further discloses that the attaching step includes the steps of generating public keys and secret keys and generating a signature for a message representing the software (page 10, see Step 1 for key generation and Step 2 for signature generation). The Biehl reference anticipates the claim as Applicant notes in the specification that the difference between the Biehl teaching and the present invention is the signature verification process (see page 15, first paragraph).

c. Regarding claim 10, which is representative of claim 14, Biehl discloses a method comprising the steps of:

obtaining a signature for the public keys from a certificate authority at the e-commerce/information service provider, the signature being generated by the certificate authority according to an undeniable digital signature scheme (page 10, Step 1 for key generation; pages 11-12, "The parameter  $p$  is used ... in the corresponding directories.");

Art Unit: 2132

providing the public keys and the signature from the e-commerce/information service provider to the user, such that the user carries out a process of verifying the signature provided from the e-commerce/information service provider to the user, interactively with the certificate authority to prove authenticity of the public keys provided by the e-commerce/information service provider (page 12, "a trusted third party ... in the corresponding directories."; page 3, "Undeniable signature schemes have the extraordinary ... check the authenticity of the message."); and

receiving an encrypted random data from the user, the encrypted random data being encrypted by the user using the public keys, decrypting the encrypted random data using the secret keys, and returning a decrypted random data to the user, such that the user checks if the decrypted random data coincides with an original random data to prove that the e-commerce/information service provider has authentic secret keys (page 9, Steps 1-4).

Biehl implicitly discloses obtaining public keys and secret keys from a certificate authority at the e-commerce/information service provider (page 10, Step 1 for key generation; pages 11-12, "The parameter  $p$  is used ... in the corresponding directories.").

d. Regarding claims 11 and 15, Biehl further discloses that the signature is generated according to an undeniable digital signature scheme based on a quadratic field (page 6, Step 1 for key generation).

e. Regarding claims 12 and 16, Biehl further discloses that the obtaining step includes the steps of generating public keys and secret keys and generating a signature

(page 10, see Step 1 for key generation and Step 2 for signature generation). The Biehl reference anticipates the claims as Applicant notes in the specification that the difference between the Biehl teaching and the present invention is the signature verification process (see page 15, first paragraph).

***Claim Rejections - 35 USC § 103***

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

6. Claim 9 is rejected under 35 U.S.C. 103(a) as being unpatentable over Biehl et al. as applied to claim 6 above, and further in view of Sims, III (6,550,011). Biehl does not disclose using different keys for different software. Sims teaches using different keys for different content which meets the limitation of software (col. 5, lines 34-37). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of Biehl to use different keys for different software, as taught by Sims, so that damage caused by one compromised key is limited to the associated software only.

7. Claims 18-20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Yoshiura et al. (6,131,162) in view of Biehl.

Art Unit: 2132

a. Regarding claim 18, Yoshiura discloses a method comprising the steps of:  
generating a signature for a hash value of a Web page of the e-commerce/information service provider at a mark manager which meets the limitation of a certificate authority (col. 7, lines 43-46; col. 31, lines 48-56);

posting the signature on a display of the Web page of the e-commerce/information service provider at a user side from the certificate authority, such that the user can initiate a process of verifying the signature (col. 31, lines 48-56; col. 32, lines 1-4); and

carrying out the process of verifying the signature at the mark manager interactively with the user in order to prove authenticity of the e-commerce/information service provider (col. 20, lines 37-40; col. 32, lines 20-25).

Yoshiura does not disclose that the Web page is a home page. However, the Yoshiura Web page shows the related individual/organization and, therefore, it meets the limitation of a home page.

Yoshiura does not disclose generating a signature according to an undeniable digital signature scheme. Biehl teaches generating a signature according to an undeniable digital signature scheme (page 1, "In 1989 Chaum and ... without the interaction of the signer."). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of Yoshiura to generate a signature according to an undeniable digital signature scheme, as taught by Biehl, so that the signature could not be verified without the interaction of the signer.



Art Unit: 2132

b. Regarding claim 19, Yoshiura does not disclose that the undeniable digital signature scheme is based on a quadratic field. Biehl discloses an undeniable digital signature scheme is based on a quadratic field (page 2, "In this paper we present ... over an imaginary quadratic field."). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of Yoshiura such that that the undeniable digital signature scheme is based on a quadratic field, as taught by Biehl. The motivation for doing so would have been that some operations for the signer have quadratic bit complexity.

c. Regarding claim 20, Biehl further discloses that the signature is generated by the steps of generating public keys and secret keys and generating a signature for the message; in this case the message is the hash value of the home page (page 10, see Step 1 for key generation and Step 2 for signature generation). The Biehl reference anticipates the claim as Applicant notes in the specification that the difference between the Biehl teaching and the present invention is the signature verification process (see page 15, first paragraph). Please refer to motivation recited for using an undeniable digital signature scheme based on a quadratic field as taught by Biehl in claim 19.

***Allowable Subject Matter***

8. Claims 1-5 are allowed. The following is an examiner's statement of reasons for allowance. The present invention is directed to a method for generating an undeniable signature based on a quadratic field. More specifically, independent claim 1 identifies the uniquely distinct steps in the signature verification process: (c2) computing a

Art Unit: 2132

response  $W$  by mapping the challenge  $C$  to the class group  $Cl(D1)$  and pulling the mapped challenge  $C$  back to the class group  $Cl(D)$  and squaring a result of mapping and pulling back, using the secret keys  $(D1, q)$ , at the signer side; and (c3) checking whether  $W = B^2$  holds or not, and judging that the signature  $S$  is legal when  $W = B^2$  holds or that the signature  $S$  is illegal otherwise, at the verifier side. The closest prior art, Biehl et al ("Efficient Undeniable Signature Schemes based on Ideal Arithmetic in Quadratic Orders"), discloses a method for generating an undeniable signature based on a quadratic field. However, the Biehl reference uses a different protocol for the signature verification process, which does not employ the specific steps mentioned above. The prior art, taken either singly or in combination, fails to anticipate or fairly suggest the limitations of applicant's independent claim, in such a manner that a rejection under 35 U.S.C 102 or 103 would be proper. The claims are therefore considered to be in condition for allowance as being novel and nonobvious over prior art.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

9. Claims 8, 13, 17 and 21 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims. The reasons for the indication

Art Unit: 2132

of allowable subject matter for these claims are the same as the reasons for allowance of claims 1-5.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Minh Dinh whose telephone number is 703-306-5617. The examiner can normally be reached on Mon - Fri: 9:00 am - 5:30 pm.


If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 703-305-1830. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

MD

Minh Dinh  
Examiner  
Art Unit 2132

MD  
6/16/2004

  
GILBERTO BARRON  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100